(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 October 2007 (18.10.2007)

PCT

(10) International Publication Number
WO 2007/117635 A3

(51) International Patent Classification:
G06F 11/30 (2006.01) *G06F 12/14* (2006.01)

(21) International Application Number:
PCT/US2007/008641

(22) International Filing Date: 6 April 2007 (06.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/789,746	6 April 2006 (06.04.2006)	US
60/789,745	6 April 2006 (06.04.2006)	US
60/789,766	6 April 2006 (06.04.2006)	US
60/789,744	6 April 2006 (06.04.2006)	US
60/789,748	6 April 2006 (06.04.2006)	US
60/789,743	6 April 2006 (06.04.2006)	US
60/789,958	6 April 2006 (06.04.2006)	US
60/789,749	6 April 2006 (06.04.2006)	US
60/824,649	6 September 2006 (06.09.2006)	US
60/828,491	6 October 2006 (06.10.2006)	US

(71) Applicant *(for all designated States except US)*: **SMOBILE SYSTEMS INC.** [US/US]; 2020 Leonard Avenue, Columbus, OH 43220 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **TUVELL, George** [US/US]; 6478 Bromfield Drive, Westerville, OH 43082 (US). **VENUGOPAL, Deepak** [IN/US]; 1220 Chambers Road, 430C, Columbus, OH 43212 (US). **HU, Guoning** [CN/US]; 3537 Chowning Ct., Columbus, OH 43220 (US).

(74) Agent: **DORTENZO, Megan**; Thompson Hine LLP, P.O. Box 8801, Dayton, OH 45401-8801 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
26 June 2008

(54) Title: MALWARE MODELING DETECTION SYSTEM AND METHOD FOR MOBILE PLATFORMS

(57) Abstract: A system and method for detecting malware by modeling the behavior of malware and comparing a suspect executable with the model. The system and method extracts feature elements from malware-infected applications, groups the feature elements into feature sets, and develops rules describing a malicious probability relationship between the feature elements. Using malware-free and malware-infected applications as training data, the system and method heuristically trains the rules and creates a probability model for identifying malware. To detect malware, the system and method scans the suspect executable for feature sets and applies the results to the probability model to determine the probability that the suspect executable is malware-infected.

WO 2007/117635 A3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US07/08641

A. CLASSIFICATION OF SUBJECT MATTER

IPC: **G06F 11/30**(2006.01),**12/14**(2006.01)
G06F 11/30(2006.01),12/14(2006.01)

USPC: 713/187,188;726/24,25

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/187,188; 726/24,25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,971,019 B1 (NACHENBERG) 29 November 2005 (29.11.2005), column 1, lines 7-11, 47-55, column 2, lines 24-57, column 8, lines 45-53, column 9, lines 25-51, column 11, lines 3-31, column 12, lines 44-52.	1,3-22,24-40 ---------- 2,23
Y	US 6,678,635 B2 (TOVINKERE et al) 13 June 2004 (13.06.2004), column 8, lines 22-30).	2, 23
A	US 2005/0229254 A1 (SINGH et al) 13 October 2005 (13.10.2005), whole document.	1-40
A	US 7,334,263 B2 (SZOR) 19 February 2008 (19.02.2008), whole document.	1-40
A	US 2004/0181664 A1 (HOEFELMEYER et al) 16 September 2004 (16.09.2004), whole document.	1-40
A	US 7,225,343 B1 (HONIG et al) 29 May 2007 (29.05.2007), whole document.	1-40

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

13 March 2008 (13.03.2008)

Date of mailing of the international search report

03 APR 2008

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Facsimile No. (571) 273-3201

Authorized officer

Ayaz Sheikh

Telephone No. 571-272-3795

Form PCT/ISA/210 (second sheet) (April 2007)